Codes over Quaternion Integers with Respect to Lipschitz Metric

Mehmet Özen, Murat Güzeltepe
Department of Mathematics, Sakarya University, TR54187 Sakarya, Turkey

Abstract

In this paper, we study codes over some finite skew fields by using quaternion integers. Also, we obtain the decoding procedure of these codes.

AMS Classification: 94B05, 94B15, 94B35, 94B60
Keywords: Block codes, Mannheim distance, Cyclic codes, Syndrome decoding

1 Introduction

Mannheim distance, which was introduced by Huber 1994, has been used in many papers up to present (for instance [1, 2, 3]). Huber defined the Mannheim distance and the Mannheim weight over Gaussian integers and, consequently, he obtained the linear codes which can correct errors of Mannheim weight one in [1]. He showed that the Mannheim distance is much better suited for coding over two dimensional signal space than the Hamming distance [1]. Moreover, some of these codes which are convenient for quadrature amplitude modulation (QAM)-type modulations were considered by Huber [1]. Fan and Gao obtained one error-correcting linear codes over algebraic integer rings [2]. The codes obtained over some finite field in [1] were extended to some finite rings [3]. In [4], Lipschitz metric was presented. Later, cyclic codes over quaternion integers were obtained in [5].

In Section 2, Lipschitz integers, also called quaternion integers, and Lipschitz distance have been considered. Also, it has been given some fundamental algebraic concepts. In Section 3, we are interested in constructing codes which are able to correct errors of quaternion Mannheim weight one. In Section 4, double error correcting codes which have minimum distance four or more are constructed and decoding procedure for these codes are given.

2 Quaternion Integers and Lipschitz Distance

Definition 1 *The Hamilton Quaternion Algebra over the set of the real numbers ($\mathcal{R}$), denoted by $H(\mathcal{R})$, is the associative unital algebra given by the following representation:*

i)$H(\mathcal{R})$ is the free $\mathcal{R}$ module over the symbols $1, i, j, k$, that is, $H(\mathcal{R}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathcal{R}\}$;

ii)1 is the multiplicative unit;
iii) $i^2 = j^2 = k^2 = -1$*;*
iv) $ij = -ji = k,\ ik = -ki = j,\ jk = -kj = i$ *[6].*

The set $H(\mathcal{Z})$, which is defined by $H(\mathcal{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k :\ a_0, a_1, a_2, a_3 \in \mathcal{Z}\}$ is a subset of $H(\mathcal{R})$, where $\mathcal{Z}$ is the set of all integers. More information which are related with the arithmetic properties of $H(\mathcal{Z})$ can be found in [6 pp. 57-71]. If $q = a_0 + a_1 i + a_2 j + a_3 k$ is a quaternion integer, its conjugate quaternion is $\overline{q} = a_0 - (a_1 i + a_2 j + a_3 k)$.The norm of q is $N(q) = q.\overline{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2$. A quaternion integer consists of two parts which are the complete part and the vector part. Let $q = a_0 + a_1 i + a_2 j + a_3 k$ be a quaternion integer. Then its complete part is a_0 and its vector part is $a_1 i + a_2 j + a_3 k$.

Definition 2 *Let $\pi \neq 0$ be a quaternion integer. If there exist $\beta \in H(\mathcal{Z})$ such that $q_1 - q_2 = \beta\pi$ then $q_1, q_2 \in H(\mathcal{Z})$ are right congruent modulo π and it is denoted as $q_1 \equiv_r q_2$ [4].*

Thus, the quotient ring of the quaternion integers modulo this equivalence is denoted as

$$H(\mathcal{Z})_\pi = \{\, q \ (\mathrm{mod}\pi)|\ q \in H(\mathcal{Z})\}\,.$$

Theorem 1 *Let $\pi \in H(\mathcal{Z})$. Then $H(\mathcal{Z})_\pi$ has $N(\pi)^2$ element [4].*

Example 1 *Let $\pi = 1 + i + j$. Then $H(\mathcal{Z})_\pi = \{0, \pm 1, \pm i, \pm j, \pm k\}$.*

Lemma 1 *Let $\pi \neq 0$ be a quaternion integer. Given $\alpha, \beta \in H(\mathcal{Z})_\pi$, then the distance between α and β is computed as $|a_0| + |a_1| + |a_2| + |a_3|$ and denoted by $d_\pi(\alpha, \beta)$, where*

$$\alpha - \beta \equiv_r a_0 + a_1 i + a_2 j + a_3 k \ (mod\ \pi)$$

with $|a_0| + |a_1| + |a_2| + |a_3|$ minimum [4].

The weight of the element γ can defined as $|a_0| + |a_1| + |a_2| + |a_3|$ and denoted by $w_{QM}(\gamma)$, where $\gamma = \alpha - \beta$ with $|a_0| + |a_1| + |a_2| + |a_3|$ minimum.

3 One Quaternion Mannheim Error Correcting Codes

Let α be an element of $H(\mathcal{Z})_\pi$ such that $\alpha^{p-1} = 1$ and let p be a prime in $\mathcal{Z}$, where $\pi = a_0 + a_1 i + a_2 j + a_3 k$ is a quaternion prime number and $p = \pi\bar{\pi}$. Then, the parity check matrix H and the generator matrix G by using the element α are obtained as follows, respectively;

$$H = \begin{pmatrix} \alpha^0 & \alpha^1 & \cdots & \alpha^{(p-1)/2-1} \end{pmatrix}, G = \begin{pmatrix} -\alpha^1 & 1 & 0 & \cdots & 0 \\ -\alpha^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ -\alpha^{(p-1)/2-1} & 0 & 0 & & 1 \end{pmatrix}.$$

Hence, the one quaternion Mannheim error correcting codes of length $n = (p-1)/2$ can be constructed by the parity check matrix H. Then the code C defined by the above parity check matrix H is able to correct any quaternion

Mannheim error of weight one. A quaternion Mannheim error of weight one takes on one of the eight values $\pm 1, \pm i, \pm j, \pm k$. The decoding algorithm for these codes is clear. Let the receive vector $r = c + e$, where the weight of the error vector e is 1 and the vector c is a codeword. Then the syndrome of the received vector r is computed $S(r) = H.r^{tr}$, where r^{tr} denote transpose of the received vector r . The value of the error is computed $S.\alpha^{-l}$, where $l(\mathrm{mod} n)$ leads how to find the location of the error, l is a nonnegative integer, and n is equal to $p - 1/2$. Notice that first we compute the syndrome of the received vector to be decoded. If the syndrome disappear in the powers of the element α, then the associates of the syndrome are checked.

We now consider a simple example with regard to the one quaternion Mannheim error correcting codes.

Example 2 *Let $\pi = 2 + i + j + k$ and $\alpha = 1 - i - j - k$. Then, we obtain the parity check matrix H and the generator matrix G by using the primitive element α of $H(\mathcal{Z})\pi$ as follows, respectively;*

$$H = \begin{pmatrix} \alpha^0 & \alpha^1 & \cdots & \alpha^{(p-1)/2-1} \end{pmatrix}, G = \begin{pmatrix} -\alpha^1 & 1 & 0 & \cdots & 0 \\ -\alpha^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ -\alpha^{(p-1)/2-1} & 0 & 0 & & 1 \end{pmatrix}.$$

Let the received vector r be $\begin{pmatrix} 1-i-j-k & 1+i & -1+i+j+k \end{pmatrix}$, then $S(r) = H.r^{tr} = 1 + i + j - k = i(1 - i - j - k) = i\alpha^1$ (See Table I), and the location of the error is found $1 \equiv 1(\mathrm{mod}3)$. The value of the error is computed as $S\alpha^{-l} = i$. So, the received vector r is corrected as $c = r - e = \begin{pmatrix} 1-i-j-k & 1 & -1+i+j+k \end{pmatrix}$.

The code, of which the parity check matrix is $H = \begin{pmatrix} \alpha^0 & \alpha^1 & \cdots & \alpha^{(p-1)/2-1} \end{pmatrix}$ can be generalized as $n = (p^r - 1)/2$. In this situation, the parity check matrix would be

$$H = \begin{pmatrix} \alpha^0 & \alpha^1 & \cdots & \alpha^{(p^r-1)/2-1} \end{pmatrix}. \tag{1}$$

The codes defined by (2) can correct errors whose quaternion Mannheim weight is equal to 1.

4 Double Error Correcting Codes

Let p be a prime in $\mathcal{Z}$ which is factored in $H(\mathcal{Z})$ as $\pi.\overline{\pi}$, where π is a prime in $H(\mathcal{Z})$. Let β denote an element of $H(\mathcal{Z})\pi$ of order $2n$. Therefore, we consider the code C defined by the following parity check matrix H:

$$H = \begin{pmatrix} \beta^0 & \beta^1 & \beta^2 & \cdots & \beta^{n-1} \\ \beta^0 & \beta^3 & \beta^6 & \cdots & \beta^{3(n-1)} \\ \vdots & & & & \\ \beta^0 & \beta^{2t+1} & \beta^{2(2t+1)} & \cdots & \beta^{(n-1)(2t+1)} \end{pmatrix} \tag{2}$$

where $t < n$ is a nonnegative integer. A word $c = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \end{pmatrix} \in H(\mathcal{Z})_\pi^n$ is a codeword of C if and only if $Hc^{tr} = 0$. If $c(x) = \sum_{i=0}^{n-1} c_i x^i$ is code polynomial, we get

$$c(\beta^{2j+1}) = 0, \text{for} j = 0, 1, \cdots, t.$$

The polynomial $g(x) = (x - \beta)(x - \beta^3) \cdots (x - \beta^{2t+1})$ is the generator polynomial of C, and $C = \langle g(x) \rangle$ is an (left or right) ideal of $H(\mathcal{Z})_\pi[x]/\langle x^n + 1 \rangle$. If multiplying the code polynomial $c(x)$ by $x(mod(x^n + 1))$, we get

$$xc(x) = c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n.$$

But we know that $x^n = -1$. Therefore, if $c(x) \in C$, then $xc(x) \in C$. Thus, multiplying $c(x)$ by $x(\text{mod}(x^n + 1))$ means the following:

i) Shifting $c(x)$ cyclically one position to the right;

ii)Rotating the coefficient c_{n-1} by π radians and locating it for the first symbol of the new codeword.

Theorem 2 *Let C be the code defined by the parity check matrix of (3). Then C is able to correct any error pattern of the form $e(x) = e_s x^s + e_t x^t$, where $0 \leq w_{QM}(e_s), w_{QM}(e_t) \leq 1$.*

Proof. Suppose that double error occurs at two different components l_1, l_2 of the received vector r . Let the error vectors be e_1, e_2, where $0 \leq w_{QM}(e_1), w_{QM}(e_2) \leq 1$. First we compute the syndrome S of r:

$$S(r) = H.r^{tr} = \begin{pmatrix} s_1 \\ s_3 \end{pmatrix}. \tag{3}$$

The polynomial $\sigma(z)$, which helps us to find the errors location and the value of the errors, is computed as follows.

$$\sigma(z) = (z - \beta^{l_1})(z - \beta^{l_2}) = z^2 - (\beta^{l_1} + \beta^{l_2})z + \beta^{l_1}.\beta^{l_2} = z^2 - (s_1)z + \varepsilon \tag{4}$$

where ε is determined from the syndromes. From $s_1 = \beta^{l_1} + \beta^{l_2}, s_3 = \beta^{3l_1} + \beta^{3l_2}$ and $\varepsilon = \beta^{l_1 + l_2}$ we get

$$s_1^3 - s_3 = 3\varepsilon\beta^{l_1} + 3\varepsilon\beta^{l_2} + \beta^{3l_2} + \beta^{3l_1} - (\beta^{3l_2} + \beta^{3l_1}) = 3\varepsilon(\beta^{l_1} + \beta^{l_2}) \tag{5}$$

from which we obtain

$$\frac{s_1^3 - s_3}{3s_1} = \frac{3\varepsilon(\beta^{l_1} + \beta^{l_2})}{3(\beta^{l_1} + \beta^{l_2})} = \varepsilon \ (\text{mod}\pi). \tag{6}$$

Thus, the roots of the polynomial $\sigma(z)$ lead us to find the locations of the errors and their values. If $\beta_1^{l_1}$ and $\beta_2^{l_2}$ are the roots of the polynomial $\sigma(z)$, then l_1 and l_2 $(modn)$ are locations of the errors. Thus, we can distinguish three situations: no error, single error, and two errors.

i) No error: $s_1 = s_3 = 0$

ii) One error: $s_1^3 = s_3 \neq 0$ (or the associates of S_1^3 is equal to the associates of s_3)

iii) Two error: $s_1^3 \neq s_3$ and $s_1 \neq 0$. (Check their associates) ■

We illustrate the decoding procedure with an example.

Example 3 *Let $\pi = 1 + 2i + 2j + 2k$ and let $\beta = 2$. Let C be the code defined by the parity check matrix*

$$H = \begin{pmatrix} 1 & 2 & -2+i+j+k & 1-i-j-k & 3 & i+j+k \\ 1 & 1-i-j-k & -1 & -1+i+j+k & 1 & 1-i-j-k \end{pmatrix}.$$

Let the codeword $c = \begin{pmatrix} 3 & 3 & 1 & 0 & 0 & 0 \end{pmatrix}$. Suppose that the received vector is $r = \begin{pmatrix} 3 & 3 & 1 & 1 & k & 0 \end{pmatrix}$. We now apply the decoding procedure for the code in Theorem 2.

1) Calculating the syndrome:

$$S = H.r^{tr} = \begin{pmatrix} s_1 \\ s_3 \end{pmatrix} = \begin{pmatrix} 1-i-j+2k \\ -1+i+j+2k \end{pmatrix} \bmod \pi.$$

One can verify that $s_3 \neq s_1^3$, which shows that two errors have occurred.

2) Calculating of the Errors Location and the Value of Errors: Using the formulas (4) and (6), we obtain

$$\begin{aligned} \varepsilon = \tfrac{s_1^3 - s_3}{3s_1} &\equiv \tfrac{-2j(-1-4i-8j-k)}{1+i} \\ &\equiv \tfrac{(-2j)(-2i)}{1+i} \\ &= -2k \equiv \beta^3\beta^4 k \pmod{\pi} \end{aligned}$$

and the roots of the polynomial $\sigma(z)$ are $\beta^3, \beta^4 k$ (See Table II). Therefore, the locations of the errors are $l_1 = 3 \equiv 3 \,(\mathrm{mod} 6)$ and its value is $(\beta^3/\beta^3) = 1$ and $l_2 = 4 \equiv 4 \,(\mathrm{mod} 6)$ and its value is $(\beta^4 k/\beta^4) = k$. Thus, one error has occurred in location 4 and its value is 1, and another one in location 5 and its value is k.

Theorem 3 *The code defined by the parity check matrix (2) has the minimum distance $d \geq 4$ if π is a prime in $H(\mathcal{Z})$ and p is a prime in $\mathcal{Z}$, where $p \geq 13$, $p = \pi.\overline{\pi}$, and t=1.*

Proof. It is sufficient to show that the decoder can distinguish single and double error for the proof. Suppose that an error of the quaternion Mannheim weight one did occur. Then $s_1^3 = s_3 \neq 0 \,(\mathrm{mod}\pi)$. From equation (4) we get

$$z_{1,2} = \frac{s_1 \pm \sqrt{\frac{s_3}{s_1}}}{2} = \frac{s_1 \pm s_1}{2}.$$

In view of Theorem 2, the decoder can distinguish between single and double errors. ■

5 Conclusions

In this paper, codes over the quaternion integer ring $H(\mathcal{Z})$ are constructed and decoding algorithms of these codes are given. These codes are constructed using a metric which is called quaternion Mannheim metric or Lipschitz metric . In addition, these codes are constructed using similar technic in [1, 2].

Table I: Powers of the element $\alpha = 1 - i - j - k$ which is root of $x^3 + 1$.

s	α^s	s	α^s
0	1	4	$-1 + i + j + k$
1	$1 - i - j - k$	5	$i + j + k$
2	$-i - j - k$	6	1
3	-1	7	$1 - i - j - k$

Table II: Powers of the element $\beta = 2$ which is root of $x^6 + 1$.

s	β^s	s	β^s
0	1	8	$2 - i - j - k$
1	2	9	$-1 + i + j + k$
2	$-2 + i + j + k$	10	-3
3	$1 - i - j - k$	11	$-i - j - k$
4	3	12	1
5	$i + j + k$	13	2
6	-1	14	$-2 + i + j + k$
7	-2	15	$1 - i - j - k$

References

[1] K. Huber., "Codes Over Gaussian Integers" IEEE Trans. Inform.Theory, vol. 40, pp. 207-216, Jan. 1994.

[2] Y. Fan and Y. Gao., "Codes Over Algebraic Integer Rings of Cyclotomic Fields" IEEE Trans. Inform. Theory, vol. 50, No. 1 Jan. 2004.

[3] M. Özen and M. Güzeltepe., "Cyclic Codes over Some Finite Rings" (submitted, 2009).

[4] C. Martinez, E. Stafford, R. Beivide and E. Gabidulin. Perfect Codes over Lipschitz Integers". IEEE Int. Symposium on Information Theory, ISIT'07.

[5] M. Özen, M. Güzeltepe, Cycliccodesoversomefinitequaternionintegerrings,J. Franklin Inst.(2010) (in press).

[6] G. Davidoff, P. Sarnak, and A. Valette., "Elementary Number Theory, Group Theory, Ramanujan Graphs", Cambridge University Pres, 2003.